AUTONOMOUS VEHICLE TECHNOLOGY—THE NEED FOR A NATIONAL STANDARD ON CYBERSECURITY

Jennifer Heemstra[†]

INTRODUCTION

Imagine, it's 4:30 p.m. on a Friday evening. You are sitting at your desk in your office, and you look down at the planner in front of you. You need to make one business call and then send an e-mail to a co-worker before you can leave the office for the weekend. You pick up your phone and dial the number for your client. As it rings, you tap the app on your watch for your autonomous car. You select "pick up" and tap the scroll down button for the "from" location. You look down the list of recently saved addresses and choose "kids' high school." You figure your two sons will be finished with their football practice before you finish your work. Once your request is sent, your car turns itself on and drives to your kids' school. A short while later as you walk out of your office building, your phone begins to ring. The Caller-ID says "your car," and you pick up the phone.

Your kids are yelling over each other about the car being hacked. Once you get them to calm down, they explain the following story. Once they entered the car, they tapped the screen located on the dashboard of the car and selected your office as their destination. They sat back with their headphones on and skimmed through Facebook posts on their phones. Shortly into the ride, the vehicle's radio turned on and began scanning through the different stations. Both of your kids played with the controls on the radio, but nothing seemed to shut it off. They assumed that a wire was loose and that they could tell you about it when they picked you up. Then, the windshield wipers activated and alternated between different speeds even though it had been sunny all day. They looked around several other vehicles who had their windshield wipers moving erratically. They tapped the screen of the car to attempt to regain control of the vehicle by switching off the auto-pilot mode, but it did not respond. As they approached the intersection where they would

[†] Ave Maria School of Law, Juris Doctorate (2018); Grand Valley State University, Bachelor of Science (2012).

normally have turned left, the vehicle suddenly made a lane change and turned right. The car began to pick up speed and was going fifteen miles-per-hour over the posted speed limit. They started to hit the screen, but again the car did not respond to any of the commands. Five minutes later, the car began to decelerate and both the radio and the windshield wipers turned off. The car slowly drifted to the side of the road and shut down. You tell your kids to keep the car off while you make arrangements for someone to pick them up. You then call 9-1-1 to report that your car was hacked while it was on auto-pilot and your kids were inside.

Although the above scenario seems to be taken out of a science-fiction or horror movie, a similar incident occurred in 2015. Andy Greenberg was driving a Jeep Cherokee when two researchers hacked into the vehicle's computer system and stalled his car on the highway.[1] Thankfully, the hack was part of a planned experiment to expose the vulnerabilities of vehicles that can connect to the internet.[2] Specifically, the two researchers used this experiment to demonstrate that they could carry out this attack from ten miles away and without physical access to the vehicle.[3] The researchers accomplished their take-over by planting a bug through the vehicle's wireless entertainment system.[4] This gave the researchers the ability to control the vehicle's functions from their home.[5]

More recently, in China, a team of scientists hacked the Tesla Model S from twelve miles away.[6] During the experiment, the researchers demonstrated they could "move the seats back and forth, trigger the [turn] indicators, wing mirrors and windscreen wipers, and open the sunroof and boot while the car was driving and in parking mode."[7] Additionally, the researchers controlled the vehicle's braking system.[8] These kinds of experiments are occurring more frequently as manufacturers begin to test their self-driving

1. Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.*

6. Olivia Solon, *Team of Hackers Take Remote Control of Tesla Model S from 12 Miles Away*, THE GUARDIAN (Sept. 20, 2016, 3:17 PM), https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes#img-1 (In addition to the experiment in China, researchers at the University of South Carolina "were able to fool the Tesla Model S's autopilot into perceiving objects where none existed or in other cases to miss a real object in the Tesla's path.").

7. *Id.*

8. *Id.*

vehicle technology.[9] Despite serious concerns regarding the security of the computers in vehicles, many individuals focus on the benefit that fully autonomous vehicles will have on society.[10]

Proponents of autonomous vehicles tout several benefits of self-driving technology.[11] Specifically, proponents argue that the technology will decrease the total number of car accidents and thereby reduce the number of fatal car accidents.[12] Additionally, daily commute times will be reduced because the vehicles will use computers to monitor the speed and flow of traffic.[13] Thus, people will spend less time in the car, and the time that individuals do spend in their cars can be used to do something other than focusing on the road.[14] Furthermore, individuals with disabilities will have more autonomy and freedom because autonomous vehicles will not rely on human input.[15] Thus, many technology and car manufacturing companies are hoping to introduce fully autonomous vehicles to the public within the next decade.[16]

---

9. Solon, *supra* note 6; *see* Greenberg, *supra* note 1.

10. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-350, VEHICLE CYBERSECURITY: DOT AND INDUSTRY HAVE EFFORTS UNDER WAY, BUT DOT NEEDS TO DEFINE ITS ROLE IN RESPONDING TO A REAL-WORLD ATTACK 6 (2016); Chris Woodyard, *McKinsey Study: Self-driving Car Yield Big Benefit*, USA TODAY, http://www.usatoday.com/story/money/cars/2015/03/04/mckinsey-self-driving-benefits/24382405/ (last updated Mar. 5, 2015, 3:57 AM); *see generally* NAT'L HIGHWAY TRAFFIC SAFETY ADMINISTRATION, *Accelerating the Next Revolution in Roadway Safety*, FEDERAL AUTOMATED VEHICLE POLICY 5–6 (Sept. 2016) (autonomous vehicles will include sensors and vehicle-to-vehicle communication capabilities, which likely will reduce the number and severity of crashes).

11. NAT'L COUNCIL ON DISABILITY, SELF-DRIVING CARS: MAPPING ACCESS TO A TECHNOLOGY REVOLUTION 16–17 (Nov. 2, 2015); *Accelerating the Next Revolution in Roadway Safety*, *supra* note 10, at 5–6; Woodyard, *supra* note 10 (Three benefits will be the reduction of time spent in the car, fewer fatalities, and more availability of parking spaces.).

12. GAO-16-350, *supra* note 10, at 6 (from 2004 to 2014 the "annual number of fatalities declined from 42, 836 . . . to . . . 32, 657." Additionally, the "NHTSA attributed 94% of highway crashes to human error in 2013, [automatic technology] could help continue the overall decline in motor vehicle fatalities over the past decade."); *Accelerating the Next Revolution in Roadway Safety*, *supra* note 10, at 5 (The NHTSA reports that 35,092 people were killed in vehicular accidents in 2015, and nearly all of these accidents were a result of "human choice or error."); Woodyard, *supra* note 10.

13. Woodyard, *supra* note 10.

14. *Id.* (Self-driving technology may allow drivers to reclaim fifty minutes of their day.).

15. Paul Stenquist, *In Self-Driving Cars, a Potential Lifeline for the Disabled*, USA TODAY (Nov. 7, 2014), http://www.nytimes.com/2014/11/09/automobiles/in-self-driving-cars-a-potential-lifeline-for-the-disabled.html?_r=0; *See generally* NAT'L COUNCIL ON DISABILITY, *supra* note 11, at 16–17.

16. Glenn Garvin, *Automakers to Sell Self-Driving Cars by the End of the Decade*, THE MIAMI HERALD (Mar. 17, 2014), http://www.govtech.com/fs/news/Automakers-to-Sell-Self-Driving-Cars-by-the-End-of-the-Decade.html?__rmid=523263753.html; Joann Muller, *The Road to Self-Driving Cars: A Timeline*, FORBES (Oct. 15, 2015, 2:52 PM), www.forbes.com/sites/joannmuller/2015/10/15/the-road-to-self-driving-cars-a-timeline/#4ee61a5e7c1b (estimating that fully autonomous vehicles will be available to the public at the earliest by 2030).

The rise of fully autonomous cars, however, raises two serious questions: 1) what are the implications of consumer liability when smart cars get into accidents, and 2) how will the automakers protect against hacking and potential cyber threats posed by this new technology. Currently, the focus of many legislators and scholars is the need for uniform legislation regarding manufacturer liability in cases where autonomous vehicles crash because the computer sensor malfunctions.[17] As of 2016, thirty-six (36) states have at least proposed legislation regarding autonomous vehicles.[18] While most of the scholarly discussion revolves around the issue of product liability, very few articles touch on issues of cyber safety.

Thus, this Note will address the current state of legislation, both foreign and domestic, on cyber safety of autonomous cars. Further, it will explore whether these legislative and administrative actions provide enough protection to consumers and the public from cyber attacks by comparing it to regulations for computer technology within nuclear power plants. Specifically, it will address whether the cybersecurity proposals are sufficient to protect against cyber attacks that will "take over" and control vehicle function.[19]

This Note has four parts. Part I will discuss the components and the foundation of the technology contained in self-driving vehicles. Part II will address the current state of the United States' legislation and efforts to create a regulatory scheme for vehicle manufacturers. Part III of this Note will address how foreign nations have attempted to produce cybersecurity regulations. Finally, Part IV will draw from the United States' nuclear regulatory committees' guideline for cybersecurity to offer a preliminary regulatory scheme that will be flexible to balance the development of self-driving vehicles and the safety of the public.

---

17. *See* John W. Terwilleger, *Navigating the Road Ahead: Florida's Autonomous Statute and its Effect on Liability*, 89-AUG. FLA. B.J. 26 (July-Aug. 2015); Roy Alan Cohen, *Self-Driving Technology and Autonomous Vehicles: A Whole New World for Potential Product Liability Discussion*, 82 DEF. COUNS. J. 328 (July 2015).

18. *Autonomous Self-Driving Vehicles*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Nov. 11, 2016), http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx#Enacted (Additionally, eight (8) states have passed statutes regarding self-driving smart cars. Furthermore, five states and Washington D.C. already allow companies to test self-driving vehicles under limited and controlled circumstances.).

19. Cyber vehicles will also likely be susceptible to attacks that will allow hackers to collect personal information from the occupant of the vehicle. For further discussion of potential cyberattacks and the privacy of autonomous vehicles *See* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA BARBARA L. REV. 1771, 1776–78 (2012).

I. TECHNOLOGICAL BACKGROUND AND CYBERSECURITY RISKS

A. Automation and Vehicle-to-Vehicle Technology

The National Highway Traffic Safety Administration (NHTSA) defines self-driving or autonomous cars as "those in which [the] operation of the vehicle occurs without direct driver input to control the steering, acceleration, and braking and are designed so that the driver is not expected to constantly monitor the roadway while operating in self-driving mode."[20] In a 2013 press release, the NHTSA described the five levels of autonomous self-driving cars and the distinguishing features between each level of automation.[21] The NHTSA affirmed the five levels and added an additional level in a subsequent policy update in September 2016.[22] Thus, autonomous vehicles fall across a six-level spectrum that focuses on the sophistication and interconnection between the technology and the vehicle.[23]

At each level, the vehicle becomes more autonomous and driver input becomes less important.[24] The lowest level of automation (Level 0) is vehicles that have no automation—in other words, the driver is the sole driving force controlling the car's functions.[25] The second level of automation (Level 1) is where certain specific control features are automatic.[26] These features include an automated electronic stability control system or pre-charged brakes.[27] The third level is Level 2, and at this level there must be automation of at least "two primary control functions designed to work in unison to relieve the driver of control of those functions."[28]

The NHTSA distinguishes Level 0–2 vehicles from Level 3–5 vehicles and designates the latter as "highly automated vehicles" or HAVs.[29] Level 3 automatic vehicles, or "limited self-driving" vehicles allow the driver to give

---

20. Press Release, Nat'l Highway Traffic Safety Administration (May 30, 2013). *See* Accelerating the Next Revolution in Roadway Safety, *supra* note 10, at 9–10 (The NHTSA defined automated vehicles systems as "a combination of hardware and software (both remote and on-board) that performs a driving function, with or without a human actively monitoring the driving environment.").

21. Press Release, *supra* note 20.

22. *Accelerating the Next Revolution in Roadway Safety*, *supra* note 10, at 10.

23. *Id.* at 9 (The NHTSA adopted the classification of autonomous vehicles from the SAE International definition of autonomous vehicles. The SAE's tier focuses on "who does what, when.").

24. *See generally id.*

25. *Id.*

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.*

the vehicle control of "safety critical functions" in certain conditions.[30] Drivers will be able to completely rely on the vehicle when they switch into the self-driving mode, but drivers can—and are expected to—take control of the vehicle when the conditions have abated.[31] Level 4 automatic vehicles will be able to control the main functions of the vehicle without human input even when a driver fails to respond to a request for intervention.[32] Drivers will have the ability to input information for navigation purposes, but there will be full automation of all safety critical functions.[33] Although in earlier stages of autonomous vehicles the NHTSA did not recognize Level 5 vehicles,[34] they recently updated their classifications to mirror the Society of Automotive Engineering (SAE) International's standard for levels of automation.[35] The SAE, and now the NHTSA, define Level 5 cars as completely autonomous and require no human input.[36] Further, these Level 5 vehicles' designs will not have steering wheels or brakes, and therefore, human drivers will not be able to take command of the vehicles.[37]

Additionally, automakers and industry leaders distinguish autonomous vehicles based on whether they are self-contained or interconnected vehicles.[38] A self-contained vehicle uses sensors to collect data about the vehicle and the external environment, and this information is then stored on the car's computer system.[39] Thus, a vehicle may be autonomous and self-contained.

Many cars on the road today have autonomous components and are self-contained.[40] The Government Accountability Office (GAO) noted that every vehicle manufactured in the model 2012 year has autonomous electronic stability.[41] In fact, many drivers have probably felt the effects of autonomous electronic stability when they have driven on icy roads or in other slippery

30. *Id.*

31. *Id.*

32. *Id.*

33. *Automated Driving: Levels of Driving Automation are Defined in New SAE International Standard J3016*, SAE INTERNATIONAL, http://www.sae.org/misc/pdfs/automated_driving.pdf (last visited Jan. 13, 2017).

34. Press Release, *supra* note 20.

35. *Accelerating the Next Revolution in Roadway Safety*, *supra* note 10, at 9.

36. SAE INTERNATIONAL, *supra* note 33; Accelerating the Next Revolution in Roadway Safety, *supra* note 10, at 9.

37. SAE INTERNATIONAL, *supra* note 33.

38. *Accelerating the Next Revolution in Roadway Safety*, *supra* note 10, at 10.

39. Glancy, *supra* note 19, at 1776–78.

40. *Id.*

41. GAO-16-350, *supra* note 10, at 6.

conditions.[42] Additionally, newer car models offer far more advanced technology such as: auto stop and start, in-car connectivity, parking assist or blind spot sensors, touchscreen infotainment, and forward-collision mitigation.[43] Thus, based on the NHTSA's autonomy spectrum, many vehicles on the road today are considered to be at least Level 2 autonomous vehicles.[44] The distinguishing feature between current vehicles and future autonomous vehicles is that many of the current vehicles lack the capacity to communicate with one another via vehicle-to-vehicle technology.

Vehicles that can communicate with other vehicles through a wireless network, in addition to gathering data from the sensors on the vehicle, are interconnected vehicles.[45] As of 2003, vehicle manufacturers and Department of Transportation (DOT) have worked to develop and implement the vehicle-to-vehicle technology.[46] The NHSTA, DOT, and car manufacturers advocate for the use of "connected technologies" systems in autonomous vehicles because these systems will increase vehicles' safety.[47] Connected vehicle-to-vehicle technology allows vehicles to communicate with each other and the environment about "imminent collisions."[48] Thus, vehicle-to-vehicle communication technology would provide better safety for autonomous vehicles because the vehicles will be able to detect potential collisions that sensor-based technologies miss.[49]

Specifically, vehicle-to-vehicle technology allows vehicles to communicate with each other about their speed or location.[50] Additionally, the vehicles can communicate with computers that are within the network such as traffic light computers.[51]

The GAO noted that a serious drawback to vehicle-to-vehicle communication systems is that they provide access points to several vehicles

---

42. *Id.* (The vehicle's sensor detects skidding and takes limited control from the driver to prevent the vehicle from skidding off the roadway.).

43. Josh Sadlier, *Must-Have Automotive Technology for 2015*, AUTOTRADER (Nov. 2014), http://www.autotrader.com/best-cars/must-have-automotive-technology-for-2015-231614.

44. *See generally* Press Release, *supra* note 20.

45. Glancy, *supra* note 19, at 1776–78.

46. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-13, INTELLIGENT TRANSPORTATION SYSTEMS: VEHICLES-TO-VEHICLES TECHNOLOGIES EXPECTED TO OFFER SAFETY BENEFITS, BUT A VARIETY OF DEPLOYMENT CHALLENGES EXIST (Nov. 2013).

47. GAO-16-350, *supra* note 10, at 19; *see generally id.*

48. GAO-16-350, *supra* note 10, at 19.

49. Will Knight, *Car-to-Car Communication*, MIT TECH. REV., https://www.technologyreview.com/s/534981/car-to-car-communication/ (last visited Mar. 10, 2017); *see* GAO-14-13, *supra* note 46, at 2.

50. GAO-16-350, *supra* note 10, at 13.

51. Glancy, *supra* note 19, at 1776–78.

at once.[52] Thus, connected vehicle technology is more susceptible to mass cyberattacks because hackers could "exploit vulnerabilities in the larger wireless networks" and use the larger wireless network to gain access to individual vehicles CAN bus systems.[53]

B. CAN Bus Systems and the Implications of Cyberattacks

Although electronic components of vehicles have been around since the 1900's,[54] they became more popular starting in the 1970's.[55] Prior to the 1980's, these electrical components were connected individually to each system with which it needed to communicate.[56] In the 1980's, car manufacturers began to place the electronic control units on a network chip.[57] These systems allowed for complex communication between electronic systems without the issues of complex wiring.[58]

Electronic control units in modern vehicles "have evolved from controlling a single vehicle function and operating in isolation from other components, to controlling multiple vehicle functions and operating in conjunction with one another" through the use of "in-vehicle communication networks."[59] These networks are called bus systems, and the most prevalent bus system in modern vehicles is the controller area network (CAN).[60] Currently, many vehicles use at least one CAN bus system, but many vehicles likely use more.[61] The CAN bus system was "designed to ensure that ECUs [electronic control units] within the vehicle could reliably and expediently

52. GAO-16-350, *supra* note 10, at 19.

53. *Id.* ("[S]ome stakeholders expressed concerns that cyber attackers could exploit vulnerabilities in the larger wireless networks used to facilitate these technologies to remotely cyberattack multiple vehicles simultaneously and take control over their safety-critical systems.").

54. Stephen A. Vincent, *Development of a CAN Based Electric Vehicle Control System*, 3–4 (June 24, 2014) (In 1900, 28% of the 4,192 vehicles in the United States "featured an electric-powered drivetrain.").

55. *Id.*; GAO-16-350, *supra* note 10, at 6–7 ("[A] vehicle manufactured in the late 1970s contained basic electronic components to meet federal regulations, and by the 1980s, the engines in most new vehicles were electronically controlled." Additionally, the electronic components of modern vehicles can control the brakes, entertainment systems, and the steering.).

56. Vincent, *supra* note 54, at 6 ("Prior to the development of CAN bus, modules often had a wired connection to every single module that they communicated with.").

57. *Id.* at 3–7.

58. *Id.* at 5–6.

59. GAO-16-350, *supra* note 10, at 7.

60. *Id.* at 7; *see also* Vincent, *supra* note 54, 3–7.

61. GAO-16-350, *supra* note 10, at 7 ("[A]utomakers may locate all ECUs on a single in-vehicle network or include one network to support safety critical vehicle functions, such as steering or braking, and another network to support convenience and entertainment systems.").

send messages to one another."[62] Industry stakeholders and researchers have noted that the CAN bus design is susceptible to cyberattacks.[63]

The CAN bus system's most significant flaw is that it is not designed to recognize whether a message was sent from a legitimate sender.[64] In fact, the system "assumes that any message . . . is sent from a trusted sender, so messages are not secured or restricted in any way."[65] As vehicles become more reliant on electronic systems and bus systems, the amount of software code also increases.[66] This increase in software increases the risks of vulnerabilities and software errors.[67] Hackers can exploit these vulnerabilities and send malicious messages through the CAN bus system to different electronic control systems.[68] As several experiments have indicated,[69] hackers can exploit the software vulnerabilities either by gaining direct, physical access to the vehicle or through remote access.[70]

The GAO found that the on-board diagnostic port was vulnerable to direct, physical attacks in the on-board diagnostics port.[71] These ports "provide . . . direct and largely unrestricted access to in-vehicle communication networks [CAN bus systems]."[72] Thus, a hacker may access "safety-critical systems" through the CAN bus by attacking the on-board diagnostics port.[73] Furthermore, the GAO noted that there are several remote access points through certain technology and telematic systems.[74] Researchers recognize "built in Bluetooth and cellular-calling capabilities" as interfaces that could be

62. *Id.* at 18.

63. *Id.* (CAN bus systems were created in the 1980's, and cyber threats were not a concern for vehicles at that time.).

64. *Id.* (Thus, a hacker may exploit the technology of self-driving vehicles to gain access to the CAN bus system and ultimately the electronic control units.).

65. *Id.* at 13.

66. *Id.* at 8–9 (The modern luxury vehicle contains about 100 million lines of software code, whereas the Boeing would only contain 6.5 million lines of code.)

67. *Id.* at 9.

68. *Id.*

69. *Id.*; Greenberg, *supra* note 1; *see also* Solon, *supra* note 6.

70. Solon, *supra* note 6; Greenberg, *supra* note 1; *see generally* GAO-16-350, *supra* note 10, at 12–13.

71. GAO-16-350, *supra* note 10, at 13 (The on-board diagnostic port is mandatory for passenger vehicles. Thus, cybersecurity plans must protect against access to the CAN bus system through these access points.).

72. *Id.*

73. *Id.* (Hackers could have access to the brakes and steering wheel through this method of direct attack on the on-board diagnostic port.).

74. *Id.*

used to launch a remote cyberattack.[75] Remote cyberattacks are more concerning than direct attacks because remote attacks allow hackers, in any part of the world, to take control of vehicles' safety-critical systems by sending messages from the access point through the CAN bus system to the safety-critical systems.[76] Additionally, remote attacks on CAN bus systems are alarming in light of the fact that the government and manufacturers wish to implement vehicle-to-vehicle technology, which makes cyber takeovers of multiple vehicles possible.[77]

The proposed vehicle-to-vehicle technology will create an inter-network between vehicles and infrastructure.[78] As self-driving technology "assume[s] control of more functions traditionally controlled by the driver such as steering and braking . . . , the systems will be tightly linked and highly responsive to inputs from external systems . . . much more so than they currently are today."[79] Thus, hackers will be able to "exploit the vulnerabilities" of the connected vehicle technology to send messages to several vehicles' CAN bus systems at once.[80] From there, the compromised vehicles' CAN bus systems will send the malicious messages to the safety-critical systems of all the vehicles on the network.[81] Unsurprisingly, several automotive industry stakeholders reported such an attack "could result in accidents or other safety impacts."[82] The threat of cyberattacks on self-driving vehicles prompted the legislature to propose several pieces of legislation aimed at facilitating the development of a cybersecurity regulation for vehicle manufacturers.[83]

II. CURRENT STATE OF UNITED STATES LAW

In July 2012, Congress passed MAP-21, which allowed the NHTSA to conduct investigations and make a report on the cybersecurity of vehicle technology.[84] Although MAP-21 was not aimed directly at creating a national guideline for autonomous vehicle manufacturers, it was one of the preliminary

75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.* at 19.
79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.*
83. Pub. L. No. 112-141 § 31402(a)(2), 126 Stat. 773 (hereinafter MAP-21); Security and Privacy in Your Car Act of 2015, S.1806, 114th Cong. (2015); Autonomous Vehicle Privacy Protection Act of 2015, H.R. 3876, 114th Cong. (2015).
84. GAO-16-350, *supra* note 10, at 11.

steps in defining the role of NHTSA in the development of emerging vehicle technology.[85] The legislation required the NHTSA to consult automotive industry stakeholders and assess emerging technology and the need for safety standards "with regard to the electronic systems in . . . motor vehicles."[86] It also required the secretary of the NHTSA to "consider the electronic components, the interaction of electronic components, the security needs for those electronic systems to prevent unauthorized access, and the effect of surrounding environments on the electronic systems."[87] Additionally, it required the NHTSA to submit a report identifying areas of vehicle electronic systems that were high priority to Senate and House Committees.[88] Thus, it paved the way for the NHTSA to regulate the security of autonomous vehicles from unauthorized access.

More recently, both the Senate and the House of Representatives introduced legislation that focused on self-driving vehicles and the cybersecurity implications.[89] Additionally, in 2016, the NHTSA released the Federal Automated Vehicles Policy that created a skeleton for future regulations.[90]

A. Privacy in Your Car Act

Senator Markey proposed the Security and Privacy in Your Car Act of 2015 (SPY Car Act of 2015) to the Senate.[91] The bill was introduced in response, in part, to car manufacturers' responses to questions regarding the security and safety of vehicles.[92] The bill provides a foundation for a federal cybersecurity guideline for autonomous vehicles. Specifically, the bill can be divided into three main parts: 1) a general guideline or standard for

85. MAP-21, *supra* note 83.

86. *Id.*

87. *Id.*

88. *Id*.

89. S.1806, *supra* note 83; H.R. 3876, *supra* note 83.

90. *Accelerating the Next Revolution in Roadway Safety*, *supra* note 10, at 11.

91. S.1806, *supra* note 83.

92. Edward Markey, *Tracking and Hacking: Security & Privacy Gaps Put American Drivers at Risk* (Feb. 2015), https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf (Senator Markey sent questionnaires to car manufacturers regarding their plans for safety and security. Senator Markey noted that the "diversity in responses . . . [by the car manufacturers] . . . show that each manufacturer is handling the introduction of new technology in very different ways, and for the most part these actions are insufficient to ensure security and privacy for vehicle consumers.").

cybersecurity, 2) cyber dashboard requirements, and 3) privacy of autonomous vehicle passengers.[93]

The bill provided a timeline for creating a standard for cybersecurity and some general guidance as to the type of regulations. The bill stated that no later than eighteen months after enactment, the committee must meet with the DOT in order to create standards for cybersecurity with autonomous vehicles.[94] Thus, all vehicles manufactured two years after the regulatory standards are finalized would be required to employ reasonable methods to prevent hacking.[95] The bill focused on three critical steps: 1) taking measures to isolate critical software programs from non-critical software programs; 2) making evaluations of the practices and measures used; and 3) adjusting cybersecurity protection and detection according to the evaluations.[96] Additionally, the vehicles must come with the ability to detect and stop cyberattacks.[97]

This bill was only a step in the legislative process and the final regulations would have been finalized three years after enactment of the bill.[98] The bill was referred to the Senate Committee on Commerce, Science, and Transportation on July 21, 2015;[99] however, the bill was not enacted.[100] Senator Markey renewed his efforts in Congress and introduced the same bill as the SPY Car Study Act of 2017.[101]

B. House of Representatives and Cybersecurity Bills

The House of Representatives have introduced a couple of bills that have required government agencies to conduct research into developing cybersecurity.[102] In January 2017, two members of the House of

93. S.1806, *supra* note 83.

94. *Id.*

95. *Id.*

96. *Id.*

97. *Id.*

98. *Id.*

99. *S.1806-SPY CAR Act of* 2015, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/senatebill/1806/committees (last visited Mar. 13, 2017).

100. *S. 1806 (114th): SPY Car Act 2015*, GOVTRACK, https://www.govtrack.us/congress/bills/114/s1806 (last visited Mar. 9, 2017).

101. *S. 680: SPY CAR Act 2017*, GOVTRACK, https://www.govtrack.us/congress/bills/115/s680 (last visited Mar. 9, 2017).

102. H.R. 701: SPY Car Study Act of 2017, GOVTRACK, https://www.govtrack.us/congress/bills/115/hr701 (last visited Mar. 10, 2017).

Representatives reintroduced the SPY Car Study Act of 2017.[103] This bill provides that the NHTSA must conduct research and determine appropriate cybersecurity regulations that should be adopted by the NHTSA and other relevant federal agencies.[104] Further, the NHTSA would be required to make two reports to the House of Representatives: the preliminary and the final report.[105] However, the likelihood of this bill being enacted is only around two percent (2%).[106]

Additionally, in November 2015, Representative Meng proposed the Autonomous Vehicle Privacy Protection Act of 2015.[107] Unlike the SPY Car Act, the Autonomous Vehicle Privacy Protection Act of 2015 did not focus on the regulation of the auto industry.

Representative Meng's bill aimed to understand the autonomous vehicle technology before it becomes a significant part of America's driving infrastructure.[108] Thus, the bill requested that the GAO conduct a study of the available technology and cybersecurity issues.[109] It required the GAO to create a public report addressing the DOT's readiness to address autonomous vehicles.[110] This bill had the same fate as the SPY Car Act and was not enacted.[111] However, the GAO did publish a 61-page report on cybersecurity initiatives that industry leaders are employing and the role of the DOT in that process.[112]

Further, the House of Representatives announced on April 28, 2016, that four House Representatives will form "the bipartisan House Smart Transportation Caucus."[113] The Caucus was created to be advocates and educators with respect to emerging vehicle technology.[114] The Caucus will

103. *Id.*

104. SPY CAR Act of 2015, H.R. 3994, 114th Cong. (2015) (While conducting the research, the NHTSA will be required to consult with "the Federal Trade Commission, the Director of the National Institute of Standards and Technology, the Secretary of Defense, the Automotive Information Sharing and Analysis Center, SAE International, manufacturers of motor vehicles, manufacturers of original motor vehicle equipment, and relevant academic institutions.").

105. *Id.*

106. H.R. 701: SPY Car Study Act of 2017, *supra* note 102.

107. H.R. 3876, *supra* note 83.

108. *Id.*

109. *Id.*

110. *Id.*

111. H.R. 3876 (114th): Autonomous Vehicle Privacy Protection Act of 2015, GOVTRACK, https://www.govtrack.us/congress/bills/114/hr3876 (last visited Mar. 10, 2017).

112. *See generally* GAO-16-350, *supra* note 10, at 8 (The modern luxury vehicle contains about 100 million lines of software code, whereas the Boeing would only contain 6.5 million lines of code.)

113. Paul Merrion, *House Smart Car Caucus Revs up Vehicle Cybersecurity Issue*, 2016 WL 1694476.

114. *Id.*

focus primarily on three issues. The Caucus is designed to "educate members about the innovation that is happening in the United States, identify policy areas that need to be improved to support the development of new technologies and boost collaboration to ensure the U.S. always maintains its competitive edge."[115] The Caucus authored the bills that were introduced in the House,[116] but otherwise has remained silent in the public since its creation.

C. GAO's Report

The GAO published a report that was based on interviews with leaders in the automotive industry, including: car manufacturers, manufactures of specific vehicle components, and scholars.[117] Although the GAO's findings do not have binding legal authority, the GAO made several suggestions regarding the role of the NHTSA and the NHTSA's role in regulating the industry. One of the GAO's findings is that there are several "key practices" that could be implemented to mitigate cybersecurity threats;[118] however, their practices have several flaws that make them currently impractical or limited in use.[119]

Two of the most frequently cited "key practices" are remote updates of software and separation between "safety-critical systems" and "non-safety-critical systems."[120] Automakers and industry leaders have frequently cited that the ability "to conduct remote, over-the-air updates of vehicle software and firmware" will be an essential piece of the automaker's ability to mitigate cybersecurity threats.[121] This technology would allow automakers to respond "quickly and effectively" to any cyberattacks that could occur.[122] Unfortunately, the implementation of remote updates is not the custom in the automotive industry.[123]

---

115. *Id.*

116. Allison Grande, *House Forms Bipartisan Caucus to Target Car Hacking Threat*, LAW 360 (Apr. 29, 2016), https://www.law360.com/articles/790794/house-forms-bipartisan-caucus-to-target-car-hacking-threat (Representative Joe Wilson and Representative Ted Lieu authored the SPY Car Study Act of 2015, which was not enacted.).

117. GAO-16-350, *supra* note 10, at 48.

118. *Id.* at 26–27.

119. *Id.*

120. *Id.*

121. *Id.*

122. *Id.*

123. GAO-16-350, *supra* note 10, at 22 ("[O]nly a few automakers have OTA update capabilities, and only one—Tesla—can update all systems . . . on a fleetwide basis remotely.").

Similarly, many of the interviewed stakeholders believe it would be possible to mitigate the effects of mass cyberattacks by separating the "safety-critical systems" and "non-safety-critical systems."[124] However, stakeholders identified two issues with separating the systems. First, it likely would be impossible to create full separation between the systems because the systems will need to be able to communicate minor things with each other.[125] Second, the ability to encrypt messages so that the CAN bus system can distinguish between messages sent from trusted sources is not available in older models.[126] CAN bus systems cannot distinguish between messages that are sent from trusted sources and non-trusted sources.[127] Further, "authentication and encryption" of messages cannot be implemented in CAN bus systems because the bandwidth is insufficient to "host these protections."[128] Thus, car manufacturers would be required to use a different network system such as Ethernet.[129] Further, the stakeholders noted that this technology must be implemented during the design process, which can take up to five years.[130]

In addition to the impracticality of the "key practices," there are several challenges that are associated with implementing cybersecurity in vehicles including: lack of transparency in the industry, cost, lack of experience, and the long design cycle.[131] The NHTSA, GAO, and the stakeholders have suggested that a multi-layer implementation of cybersecurity will be most effective at preventing cyberattacks.[132] Although the NHTSA and automakers have formed groups which would allow people to share their information, vulnerabilities are still found.[133] One such vulnerability is that when automakers place orders with the part suppliers, many of the automakers do not include sufficient information or context on how the individual part works with the larger system.[134] Additionally, industry leaders are afraid of a prescriptive law that requires certain regulations because technology advances at a relatively fast pace.[135]

---

124. *Id.* at 2, 26–27.
125. *Id.* at 21.
126. *Id.*
127. *Id.*
128. *Id.*
129. GAO-16-350, *supra* note 10.
130. *Id.*
131. *Id.*
132. *Id.*
133. *Id.*
134. *Id.* at 25–26.
135. GAO-16-350, *supra* note 10, at 39.

D. National Highway Traffic and Safety Administration's Reports

The NHTSA is responsible for "setting and enforcing safety performance for motor vehicles and motor vehicle equipment."[136] In addition, MAP-21 authorized the NHTSA to consider the need for safety standards of emerging technology and how to prevent "unauthorized access" to electronic systems.[137] Thus, the NHTSA has authority to create regulations and guidelines for technology companies and the auto industry with regards to the production of autonomous vehicles.

Recently, the NHTSA has taken an active role in creating a guideline and recently published a Federal Automated Vehicle Policy;[138] however, the policy is not intended to be the final guideline or regulation.[139] The NHTSA stated that more research was necessary before the final regulatory standard would be proposed and enacted.[140] Thus, the NHTSA stated that its intention in creating the policy is to create a foundation and basic framework for future regulations.[141]

According to the report, the DOT anticipates that reports and guidelines offered by the NHTSA and the industry standards will provide manufacturers with enough guidance to ensure that autonomous vehicles—particularly the HAVs—have security systems that will be "reasonably safe under real-world conditions."[142] Although the focus of the NHTSA's guideline is the HAVs,[143] the NHTSA notes that the guidelines should be applied to Level 0–2 autonomous vehicles.[144]

The NHTSA's policy delves into several areas of autonomous vehicles. Particularly, the NHTSA states that each manufacturer should ensure that "it

---

136. *Who We Are and What We Do*, NHTSA, https://www.nhtsa.gov/About-NHTSA/Who-We-Are-and-What-We-Do (last visited Dec. 9, 2016) (The NHTSA was established in 1970 through the Highway Safety Act of 1970. The NHTSA serves several functions, including: 1) setting and enforcing safety regulations for motor vehicles and motor vehicle equipment and 2) conducting research into defects and safety of motor vehicle equipment.).

137. MAP-21, *supra* note 83.

138. Accelerating the Next Revolution in Roadway Safety, *supra* note 10.

139. *Id*. at 3–6.

140. *Id*. at 21.

141. *Id*. at 3–6. The policy is an "initial step" in determining testing procedures and standards for autonomous vehicles (The NHTSA and manufacturers will continue to test these procedures and guidelines, and share the information and data collected from the tests with the "government, industry, and public.").

142. *Id*. at 11.

143. *See generally id*. at 11–31.

144. *Id*. at 31 (The NHTSA states "most of the [g]uidance . . . and considerations specified under . . . 'Vehicle Cybersecurity' should generally apply to the full spectrum of automated vehicle systems.").

has applied appropriate functional safety and cybersecurity practices."[145] The NHTSA will assess the level of security and safety of the autonomous vehicles by reviewing manufacturers' reports.[146] These reports will be voluntary and will discuss how the NHTSA's guidance was incorporated in the production of the vehicles.[147]

Further, the NHTSA's policy enumerates several areas that the report should cover, with one aspect being the vehicle's cybersecurity.[148] The NHTSA states that for vehicles already being tested, the safety assessments must be provided "within four months after completion of the PRA [Paperwork Reduction Act] process."[149] Additionally, the NHTSA notes that in the future they may be able to request more information or modify the information required from manufacturers regarding how the manufacturer incorporated the guidelines into the manufacturer's cybersecurity plans.[150] As noted earlier, this letter will be voluntary; however, the NHTSA notes that this policy may be refined and become mandatory for manufacturers through future rules.[151] Although most of the policy was effective on the policy's publication date, the requirement for the report will "not take effect until after NHTSA completes the process required by the [PRA]."[152]

Additionally, the NHTSA specifically addresses autonomous vehicle safety in half a page, and it suggests that autonomous vehicle manufacturers follow a "robust product development process" to minimize cybersecurity concerns.[153] The NHTSA's policy emphasizes the role of industry organizations in the development of cybersecurity regulations.[154]

In one of the few mandatory portions of the guidelines, the NHTSA states that the process of incorporating the cybersecurity "should be fully documented and all actions, changes, design choices, analyses, associated testing and data should be traceable within a robust document version control environment."[155] Additionally, the NHTSA "envisions" that software updates

145. *Accelerating the Next Revolution in Roadway Safety*, *supra* note 10, at 11.

146. *Id.* at 16.

147. *Id.*

148. *Id.* at 15 (The NHTSA's safety assessment report covers fifteen various areas regarding the vehicle's ability to function on roads, safety, and local and state laws. Only a small portion of the report is dedicated solely to cybersecurity of the vehicle.).

149. *Id.*

150. *Id.* at 16.

151. Accelerating the Next Revolution in Roadway Safety, *supra* note 10, at 15.

152. *Id.* at 16.

153. *Id.* at 21 (including an on-going monitoring and risk assessment of the system).

154. *Id.*

155. *Id.*

will be made available by the manufacturers through "remote updates or other means."[156] If there is a change to the updates, the NHTSA expects that the manufacturers will update their safety assessment letter.[157] Thus, the NHTSA is pushing for full documentation, even if the safety assessment letter is voluntary.

Furthermore, the NHTSA strongly emphasized the necessity of reporting known vulnerabilities at each level of the production.[158] The NHTSA warned "[e]ach industry member should not have to experience the same cyber vulnerabilities in order to learn from them."[159] Thus, the NHTSA's preliminary guidelines are to ensure that everyone in the industry is informed about vulnerabilities rather than actually implementing protocols or standards for car manufacturers to meet; however, as noted by the GAO the industry leaders believe the communication between industry leaders at various steps in the chain of production is not as effective as it could be.[160] Without a mandatory provision requiring communication, the NHTSA's request is merely a suggestion, which could easily be disregarded by industry leaders.

The NHTSA notes that the guidelines are not mandatory; however, the NHTSA states that some regulations can be enforced through the tools already available to the NHTSA.[161] Of the tools available, two are especially important in the implementation of a cybersecurity standard.

First, the legislature has granted the NHTSA the authority to enforce vehicle regulations. This enforcement authority is broad, and the NHTSA has extended the authority to cover vehicle-to-vehicle technology and self-driving technology. The most useful aspect of this authority is that manufacturers of vehicles are still required to comply with the NHTSA's authority to recall vehicles and the NHTSA's "authority to address defects that pose unreasonable risks to safety."[162] As the NHTSA conducts more research on vehicle-to-vehicle technology and self-driving technology, the NHTSA can publish their findings regarding the safety of the vehicle technology and suggestions that will guide manufacturers to alleviate the risks.

---

156. *Id.* at 15.

157. *Accelerating the Next Revolution in Roadway Safety*, *supra* note 10, at 16.

158. *See generally id.* at 21–22.

159. *Id.*

160. GAO-16-350, *supra* note 10, at 21.

161. *See Accelerating the Next Revolution in Roadway Safety*, *supra* note 10, at 48 ("The NHTSA has four primary tools. . . : Letters of interpretation; Exemptions from existing standards; Rulemakings to amend existing standards or create new standards; and Enforcement authority to address defects that pose an unreasonable risk to safety.").

162. *Id.* at 11, 48.

Second, the NHTSA may amend its existing standard or create new standards.[163] This process may be started by an outside party or by the NHTSA.[164] While this tool is the most time consuming, the NHTSA notes that this tool allows it to make the most comprehensive changes.[165] Thus, this tool will be most beneficial in the future because the NHTSA will be able to create new regulations that reflect the results of the NHTSA's and industry leaders' research with regards to the emerging technology and its associated risks.

Congress has introduced several bills aimed at authorizing the NHTSA to conduct research and establish a preliminary standard for cybersecurity; however, none of the bills have been enacted.[166] Similarly, the NHTSA issued a policy statement regarding cybersecurity, which is admittedly a simple framework for the future.[167] Additionally, the NHTSA suggests manufacturers follow industry standards regarding cybersecurity guidelines, but as noted in the GAO report, there are issues of effective communication among industry members.[168] The United States' auto industry is practically unregulated with regards to the cybersecurity systems. Thus, legislators and the NHTSA should renew their efforts and draw guidance from security standards that have already been implemented.

III. CURRENT STATE OF FOREIGN LAW

One area that may be informative as the race for autonomous vehicles becomes more intense, would be foreign countries' policies on autonomous vehicles and cybersecurity. The introduction of autonomous vehicles generated an international race to become the first country to have commercial autonomous vehicles. Like much of the proposed legislation in the United States, the development of autonomous vehicle legislation in these countries have focused primarily on products liability in case of accidents. Further, several countries have promulgated regulations regarding when the autonomous vehicles can be tested, the level of control of drivers, and similar

163. *Id.* at 3–6.
164. *Id.*
165. *Id.*
166. S.1806, *supra* note 83; *see* H.R. 3876.
167. *Accelerating the Next Revolution in Roadway Safety*, *supra* note 10, at 3–6.
168. GAO-16-350, *supra* note 10.

matters.[169] In some instances, however, the development of foreign law on autonomous vehicles is hindered because it may not be permitted within their country.[170]

Although several nations have conducted interviews and experiments regarding autonomous vehicles, many have opted to postpone creating regulatory schemes regarding cybersecurity until they have conducted further experiments on the technology.[171] For example, the United Kingdom's Department of Transportation published a report that stated the current legislation and regulations will likely be appropriate to handle the cyberthreats; however, an examination of the U.K.'s existing regulatory framework will be completed by the end of 2018.[172]

Similarly, Korea's Director General of the Motor Vehicle Management published a policy for autonomous vehicles.[173] Although lacking in specifics, the policy addresses several areas of cybersecurity which will be enhanced.[174] Additionally, the policy provides that a cybersecurity guideline would likely be drafted in 2016, and by the year 2018, existing standards will be revised to incorporate the 2016 guideline.[175]

Likewise, Germany's legal structure focuses on liability for manufacturers in the event of a crash.[176] German industry leaders have been experimenting with technology and creating a standard for cybersecurity.[177] Similar to the efforts led by United States' automakers, German automakers are working

---

169. *See Germany to Create World's First Highway Code for Driverless Cars*, NEW SCIENTISTS (Sept. 21, 2016), https://www.newscientist.com/article/mg23130923-200-germany-to-create-worlds-first-highway-code-for-driverless-cars/.

170. *Vienna Convention on Traffic Safety*; Art. 8(1), (5) (One issue that foreign nations may have in determining whether to allow autonomous vehicles in their country is that the Vienna Convention on Traffic Safety requires "[e]very moving vehicle . . . shall have a driver" that "shall at all times be able to control his vehicle." Thus, these countries must determine first if fully autonomous vehicles are even permitted because of the treaty.).

171. Department for Transport, *The Pathway to Driverless Cars Summary Report and Action Plan* (Feb. 2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401562/pathway-driverless-cars-summary.pdf; Yong Seog Kim, *Autonomous Vehicle Policy* 6 (May 23, 2016), http://www.ircobi.org/wordpress/downloads/ad-session-seoul.pdf.

172. Department for Transport, *supra* note 171, at 28.

173. Kim, *supra* note 171, at 6.

174. *Id.* at 10.

175. *Id.*

176. Germany to Create World's First Highway Code for Driverless Cars, *supra* note 169 (The proposal requires vehicles with auto-pilot to have a black box installed. This would allow investigations to determine what happened in the event of a crash.).

177. *Id.*

with the International Organization of Standardization to create a voluntary standard that will focus on cybersecurity.[178]

Thus, the ability to compare U.S. regulations on cybersecurity measures to foreign nations is somewhat difficult; however, since the United States is unlikely to enact any regulations before 2018, the United States may be able to draw from the guidelines enacted by the United Kingdom, Germany, or Korea to fashion a cybersecurity guideline for U.S. automakers. On the other hand, autonomous vehicles are already in production and will be on the market by 2020. Thus, the United States should draw upon similar domestic regulations that will allow the United States to regulate the industry sooner.

IV. THE APPLICABILITY OF NUCLEAR POWER PLANT CYBERSECURITY TO SELF-DRIVING VEHICLE TECHNOLOGY

Since the United States and other sovereign nations have yet to establish a cybersecurity framework, likely the most effective approach is to look outside of the realm of autonomous vehicles to other cyber regulations. Specifically, it would be beneficial to look at industries that are highly regulated because of the significant threats they pose to public safety.

A. The United States Nuclear Regulatory Cybersecurity Regulations

After September 11, 2001, the U.S. Nuclear Regulatory Committee (NRC) codified a cybersecurity regulation.[179] This standard is touted as the highest standard for any American industry.[180] Many of the U.S. NRC's guidelines, however, can be incorporated within the NHTSA's autonomous vehicle guidelines because of their flexibility.

The guideline focuses on protecting computer systems from three main forms of cyberattacks: 1) attacks that will give the hacker access to the confidential and private information, 2) attacks that will "deny access to systems, services, and/or data," and 3) those that will impact the operation of the nuclear power plant.[181]

One of the U.S. NRC's mandatory requirements for nuclear power plants is that proper plants must provide a cybersecurity plan for the NRC's review

178. GAO-16-350, *supra* note 10, at 30.

179. *Issues and Policy*, NEI, https://www.nei.org/Issues-Policy/Safety-and-Security/Plant-Security (last visited Mar. 13, 2017).

180. *Id.*

181. 10 CFR § 73.54(a)(2)(i)–(iii) (2015).

and approval.[182] In the report, the nuclear power plants provide "high assurance" that the computer networks and data have protection against cyberattacks.[183] Specifically, the NRC requires the cybersecurity plan to focus on the network and computers that are involved or related to "(i) safety-related functions and important-to-safety functions[,] (ii) security functions[,] (iii) emergency preparedness functions . . . [,] and (iv) support systems, which if compromised, would adversely impact safety, security, or emergency preparedness functions."[184] Although, the U.S. NRC does not define "high assurance" the committee has defined "reasonable assurance" as: the recognition that "adequate protective measures can and will be taken in the event of a[n] . . . emergency."[185] Reasonable assurance is based on licensees complying with NRC regulations and guidance, as well as licensees and offsite response organizations demonstrating that they can effectively implement emergency plans and procedures during periodic evaluated exercises.[186]

Thus, the guideline allows power plants the flexibility to determine their own cybersecurity plan, while also allowing the NRC the ability to test the plan in a controlled evaluative exercise.[187]

Additionally, the U.S. NRC makes communication between the various contractors and industry leaders mandatory.[188] The U.S. NRC's policy requires that those seeking licenses "ensure that . . . contractors[ ] are aware of cybersecurity requirements and receive the training necessary to perform their assigned duties and responsibilities."[189] Further, the NRC requires that the cybersecurity plan cover include a description of how the nuclear power plant will: "maintain the capability for timely detection and response to cyberattacks; mitigate the consequences of cyberattacks; correct exploited vulnerabilities; and restore affected systems, networks, and/or equipment affected by cyberattacks."[190]

B. Application of the Nuclear Regulatory Committee's Cybersecurity

182. *Id.* § 73.54.

183. *Id.* § 73.54(a).

184. *Id.* § 73.54(a)(1)(i)–(iv).

185. *FREQUENTLY ASKED QUESTIONS ABOUT EMERGENCY PREPAREDNESS AND RESPONSE*, U.S. NRC, https://www.nrc.gov/about-nrc/emerg-preparedness/faq.html#8 (last updated Dec. 21, 2016).

186. *Id.*

187. *Id.*

188. 10 CFR § 73.54(d)(1) (2015).

189. *Id.*

190. 10 CFR § 73.54(e)(2)(i)–(iv) (2015).

Guideline to Autonomous Vehicles

The push to form regulatory standards is important for autonomous vehicles. It is essential to the creation of a secure infrastructure. Current laws allow manufacturers to sell automated vehicles even though there are no regulations or standards in effect.[191] Further, the process of manufacturing and producing vehicles begins about five years before the vehicle will be available for public use on the road.[192] Thus, the development of cybersecurity and guidelines is imperative. Based on the GAO's recommendations, the U.S. NRC's guideline for nuclear power plants, and the NHTSA's current enforcement tools, the NHTSA could implement a strong cybersecurity system, which allows for the growth of the self-driving vehicle market and promotes strong cybersecurity for vehicles.

Under the finalized regulatory scheme, the NHTSA should use its existing enforcement tools to change its standard and make cybersecurity reports mandatory like the U.S. NRC code.[193] Similar to the U.S. NRC code, the NHTSA does not have to mandate (at least not until there is more research) a specific cybersecurity system that must be utilized by the auto-industry; however, automakers' plans should detail how the NHTSA's guidelines and industry standards have been incorporated into the vehicles' design.[194] Additionally, it should offer reasonable assurance that vehicles have cybersecurity that will allow the manufacturers to detect cyber threats in real-time.[195] Manufacturers' reports should include information regarding how the manufacturers will detect, mitigate, and prevent cyberattacks from occurring.[196] Additionally, manufacturers should also be required to show how they are prepared to "implement emergency plans . . . during evaluated exercises."[197] This would allow the NHTSA the proper oversight over the production of vehicles while allowing manufacturers the opportunity to develop new technology.

---

191. Accelerating the Next Revolution in Roadway Safety, *supra* note 10, at 11 (including an on-going monitoring and risk assessment of the system. Under our current legal system, the manufacturers self-certify that the vehicles they manufacture for public use comply with all applicable Federal Motor Vehicle Safety Standards (FMVSS).).

192. GAO-16-350, *supra* note 10, at 6.

193. *See generally* 10 CFR § 73.54 (2015).

194. *See id.*

195. GAO-16-350, *supra* note 10, at 30; 10 CFR § 73.54(a) (2015).

196. 10 CFR § 73.54(e)(2)(i)–(iv) (2015).

197. *Frequently Asked Questions About Emergency Preparedness and Response*, *supra* note 185.

Additionally, the NHTSA should mandate that companies involved in any stage of the self-driving vehicle production cycle understand the cybersecurity requirements necessary for the specific parts as well as the entire vehicle.[198] Specifically, automakers should be required to provide specific information to part suppliers regarding the use of the parts in the entire vehicle system. This would reduce the current risk that vulnerabilities will be found at the interfaces where software codes meet as well as further the production of cyber-safety technologies in the vehicles.[199]

The NHTSA should also begin research on using Ethernet as opposed to CAN bus systems in vehicles. This would allow for better encryption of messages sent between electronic control units.[200] Regardless of the network used, the NHTSA should also mandate that manufacturers have a team of engineers and programmers that can assist in the case of an emergency. These should be the same teams that will demonstrate how vehicles will react in the "evaluated exercises."[201] They will have the opportunity to stop cyberattacks as soon as they are detected and create new software that will prevent similar cyberattacks from happening.

Finally, the NHTSA could also use its existing power to create new regulations and require car manufacturers to obtain cyber insurance policies. Cyber insurance policies would allow the manufacturers to mitigate the damages from a variety of cyber attacks.[202] In addition to covering first-party costs, the cyber insurance policies can include third-party coverage, which will benefit the consumers.[203] Although this will not prevent cyberattacks from occurring, manufacturers can use this to "mitigate the damages of cyber attacks."[204]

The NHTSA already has several tools that serve as a foundation for the new regulatory scheme such as the NHTSA's authority to recall vehicles that pose unreasonable risks due to defects in the vehicle. As the NHTSA and the manufacturers test the effectiveness of these tools, the NHTSA can recall vehicles that have high susceptibility to cyber attacks. There are, however,

198. GAO-16-350, *supra* note 10, at 30; *see* 10 CFR § 73.54 (2015).

199. GAO-16-350, *supra* note 10, at 30.

200. *Id.*

201. *Frequently Asked Questions About Emergency Preparedness and Response*, *supra* note 185.

202. Natalie A. Baughman, WITH SELF-DRIVING VEHICLES ON THE FOREFRONT, COMPANIES SHOULD CONSIDER CYBER SECURITY INSURANCE, THE NAT'L LAW REV. (Feb. 17, 2015) (The cybersecurity insurance should protect against "data breaches, business interruptions, and network damage.").

203. *Id.* (The first-party coverage would cover costs such as: notifying customers, forensic services to determine the source of the breach, fixing the computers and/or network. In addition, these policies also would allow third parties to recover costs for reimbursement expenses.).

204. *See* 10 CFR § 73.54(e)(2)(ii).

some regulations that will be beneficial in the development of autonomous vehicles that draw from the GAO's report and the U.S. NRC's code for cybersecurity for nuclear power plants.

CONCLUSION

Vehicle technology has evolved significantly in the past decade. Although the legislature has authorized the NHTSA to research the developing technology, the federal government has not proposed a guideline for cybersecurity or regulations. Understandably, the NHTSA and auto industry leaders wish to avoid strict prescriptive laws because technology and cyber threats are constantly evolving; however, the potential for significant damage to the public safety is a growing concern and should be addressed with a flexible guideline.

The NHTSA should draw on domestic industries that have cybersecurity regulations to form a flexible regulation. Particularly, the NHTSA can draft mandatory provisions that require communication among auto manufacturers and part manufacturers. Thus, the security systems will not have gaps in their code. Additionally, a mandatory reporting requirement would be more beneficial than the voluntary system. This would allow the NHTSA to review and thoroughly inspect the manufacturers' compliance with the guidelines. Similarly, a mandatory requirement that vehicles move away from the CAN bus system to a more secure network system would also be beneficial.

This Note has shown the susceptibility of CAN bus systems and vehicle-to-vehicle technology (both of which will be highly utilized in future self-driving vehicles) and a potential source that the legislature could use to form a flexible regulatory guideline for cybersecurity. Since manufacturers believe vehicles with auto-pilot abilities (Level 3 automation) will be available starting in 2020, it is imperative that the legislature or the NHTSA take more steps towards forming a cybersecurity regulation that will further the development of autonomous vehicles and protect the public.